Number Theory Fall 2009
Homework 10
Due: Wed. Nov. 11, start of class

9.2 Statement of quadratic reciprocity

Exercise 9.1. *Use quadratic reciprocity to determine for which primes p is 7 a square mod p.*

9.3 Euler's criterion

Exercise 9.2. *Show $\square_p$ is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$. Show the map $\sigma : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})$ given by $\sigma(x) = x^2$ is 2-to-1. Conclude the subgroup $\square_p$ has index 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$, i.e., $|\square_p| = \frac{p-1}{2}$.*

Exercise 9.3. *Explicitly write down the values of $\left(\frac{\cdot}{p}\right)$ for $p = 7, 11, 13$. In each case, write down what the subgroup $\square_p$ of $(\mathbb{Z}/p\mathbb{Z})^\times$ is.*

9.4 The value of $\left(\frac{2}{p}\right)$

Exercise 9.4. *Let $a, b \in \mathbb{N}$. Show for p prime*

$$(a+b)^p \equiv a^p + b^p \text{ mod } p.$$

9.5 The story so far

Exercise 9.5. *Compute $\left(\frac{24}{61}\right)$, $\left(\frac{30}{61}\right)$, and $\left(\frac{31}{61}\right)$.*

9.7 The full Chinese remainder theorem

Exercise 9.6. *Let $\gcd(m, n) = 1$ and $\alpha : (\mathbb{Z}/mn\mathbb{Z}) \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ be given by $\alpha(a, b) = (a \text{ mod } m, b \text{ mod } n)$. Check that $\alpha(0) = (0, 0)$, $\alpha(1) = (1, 1)$, $\alpha(a + b) = \alpha(a) + \alpha(b)$ and $\alpha(ab) = \alpha(a)\alpha(b)$. This means α is a* ring homomorphism.

Exercise 9.7. *Exercises 9.7.1, 9.7.2.*